(19)日本国特許庁（ＪＰ）　(12)公開特許公報(A)　(11)特許出願公開番号
特開2003－167805
（P2003－167805A）
(43)公開日　平成15年6月13日(2003.6.13)

(51)Int.Cl.[7]	識別記号	Ｆｉ		ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　13/00	３５３	Ｇ０６Ｆ　13/00	３５３Ｃ	５Ｂ０８９
Ｈ０４Ｌ　12/46	２００	Ｈ０４Ｌ　12/46	２００Ｘ	５Ｋ０３３

審査請求　有　　請求項の数7　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－370464(P2001－370464)

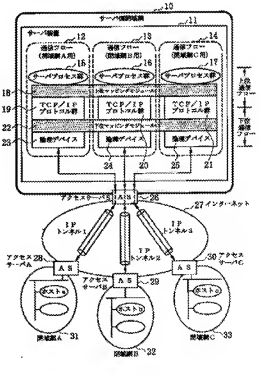
(22)出願日　平成13年12月4日(2001.12.4)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　吉良　雄介
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　小野　諭
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100077274
弁理士　磯村　雅俊　（外１名）

最終頁に続く

(54)【発明の名称】　複数ユーザ閉域網とサーバ閉域網間のネットワーク通信方法およびサーバ装置

(57)【要約】
【課題】サーバ閉域網の物理的に１台のサーバ装置を，各ユーザ閉域網間で共有せず，各ユーザ閉域網に独立して提供することで，専用サーバとしての動作をさせる。
【解決手段】複数ユーザ閉域網３１～３３は、サーバ側閉域網１０とＩＰトンネルを用いてアクセスサーバ２６，２８～３０により接続を行う。接続要求があると、アクセスサーバ２６はどの閉域網の要求かを識別し、ユーザ閉域網に固有の識別符号をパケットタグ付けし、サーバ装置１１に転送する。サーバ装置１１は、プロトコルスタック１９～２１までの上位通信フローと、プロトコルスタック１９～２１から論理デバイスインタフェース２３～２５までの下位通信フローを複数備え、これらの通信フロー１２～１４をユーザ閉域網３１～３３に割り当てる。サーバ装置１１は、受信したパケットの識別タグから送信元ホストの閉域網を特定する。



1

【特許請求の範囲】

【請求項１】　複数のユーザ側閉域網とＩＰトンネルを用いてアクセスサーバにより接続を行うサーバ側閉域網内に物理的に１台のサーバ装置を用いた網間ネットワーク通信方法であって、

サーバプロセス群とプロトコルスタックとの組み合わせを記憶し、かつ前記サーバプロセス群とプロトコルスタックとのリンクを記憶した内容に従って制御するモジュールにより管理される上位通信フローと、物理ネットワークインタフェースまたは論理デバイスインタフェースと前記プロトコルスタックとの組み合わせを記憶し、かつ前記プロトコルスタックを該当する物理ネットワークインタフェースまたは論理デバイスインタフェースにリンクさせるモジュールにより管理される下位通信フローとの組み合わせからなる通信フローを複数用意し、

前記通信フローをユーザ側閉域網ごとに１つずつ割り当てることにより、各ユーザ側閉域網と前記サーバ装置間における前記サーバ装置内の個々の通信経路をネットワーク上、論理的に分離することを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項２】　請求項１に記載のネットワーク通信方法において、

前記通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースにネットワークを介して接続する各ユーザ側閉域網との通信では、当該通信フローのプロトコルスタックとサーバプロセス群とを用いて各ユーザ側閉域網に独立したサーバサービスの提供を行うことを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項３】　請求項１または２に記載のネットワーク通信方法において、

前記複数の通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースに対し、ＩＰアドレスの重複した割り当てを許容することを特徴とする複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法。

【請求項４】　複数のユーザ側閉域網とＩＰトンネルを用いてアクセスサーバにより接続を行うサーバ側閉域網に設けられる物理的に１台のサーバ装置であって、

サーバプロセス群とプロトコルスタックとの組み合わせを記憶し、かつ前記サーバプロセス群とプロトコルスタックとのリンクを記憶された内容に従って制御することにより、上位通信フローを管理する手段と、

物理ネットワークインタフェースまたは論理デバイスインタフェースと前記プロトコルスタックとの組み合わせを記憶し、かつ前記プロトコルスタックを該当する物理ネットワークインタフェースまたは論理デバイスインタフェースにリンクさせることにより、下位通信フローを管理する手段と、

上位通信フローと下位通信フローとの組み合わせからなる通信フローを複数装備し、前記通信フローをユーザ側閉域網ごとに１つずつ割り当てることにより、各ユーザ側閉域網と前記サーバ装置間における前記サーバ装置内の個々の通信経路をネットワーク上、論理的に分離する通信手段とを具備することを特徴とするサーバ装置。

2

【請求項５】　請求項４に記載のサーバ装置において、

前記通信フローごとの物理ネットワークインタフェースまたは論理デバイスインタフェースにネットワークを介して接続を行う各ユーザ側閉域網との通信では、当該通信フローのプロトコルスタックとサーバプロセス群とを用いて、各ユーザ側閉域網に独立したサーバサービスを行う仮想サーバ提供手段を具備することを特徴とするサーバ装置。

【請求項６】　請求項４または５のいずれかに記載のサーバ装置の動作をコンピュータに実現させるためのサーバ装置用プログラム。

【請求項７】　請求項６に記載のサーバ装置用プログラムを格納したことを特徴とするコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、インターネットやプライベートネットワークを介して接続された複数の異なる閉域網間での通信を行うエクストラネット向けのアプリケーションホスティングサービスや情報共有サーバサービスなどのネットワーク通信方法およびその装置に関し、例えば物理的に１台のサーバを用いて複数のユーザ側閉域網にアプリケーションを提供するサーバサービスや、サーバを介してファイルやデータベースなどを複数のユーザ側閉域網に共有化するサービスを行うための複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法およびサーバ装置に関する。

【０００２】

【従来の技術】インターネットを始めとするネットワーク通信の利用は広く普及しており、企業やコミュニティなどは通信コストを安く抑えかつ安全な通信を行うために閉域網を利用してイントラネットやエクストラネットを構築している。また、近年、閉域網は大企業のみならず中小企業やＳＯＨＯ（Ｓｍａｌｌ　Ｏｆｆｉｃｅ　Ｈｏｍｅ　Ｏｆｆｉｃｅ）でも用いられており、その数は増加の傾向にある。さらに、閉域網を用いてＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）内ＬＡＮ（例えば、イントラネットの中にさらに階層的なネットを構築した形態）を構築する等、閉域網の利用形態も多様化している。

【０００３】このような小規模多数化している閉域網にサーバサービスを提供する方法として各閉域網にサーバを設置する方法があるが、コストや稼働がかかりサーバを設置する側の負担が大きい。そこで、物理的に１台のサーバを用いて各閉域網にサーバサービスを行うので

あるか、インターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立した提供を可能にして、各閉域網にそれぞれ専用サーバがあるかのような動作を可能にする仮想プライベートサーバの構築を考えることにする。

【０００４】閉域網の構築には、グローバルアドレスの取得に手間とコストがかかるために、ローカルアドレスを用いる方法が多く採用されている。このように構築されている複数の閉域網に対して、物理的に１台のサーバを用いてサーバサービス提供を考えた場合、次のような問題の解決が必要となる。

（１）サーバ側閉域網を含めた閉域網間でのローカルアドレス空間の競合

（２）サーバを介して他の閉域網をまたぐ等の不正アクセス

（３）サーバから各閉域網内にあるホストへの接続の確立

（４）サーバ側を含む閉域網の追加や網構成変更の容易性

【０００５】複数のユーザ側閉域網とサーバ側閉域網との間で通信を行うための従来技術としては、Ｌ２ＴＰ（Ｌａｙｅｒ ２ Ｔｕｎｎｅｌｉｎｇ Ｐｒｏｔｏｃｏｌ）やＩＰｓｅｃ（ＩＰ ｓｅｃｕｒｉｔｙ ｐｒｏｔｏｃｏｌ）などに代表されるＩＰ（Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌ）トンネル技術、ＮＡＴ（Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）やＲ－ＮＡＴ（特願２００１－０１６２５５号公報参照：Ｒｏｏｔ ｓｉｄｅ－Ｎｅｔｗｏｒｋ Ａｄｄｒｅｓｓ Ｔｒａｎｓｌａｔｉｏｎ）に代表されるアドレス変換技術、さらにＩＰトンネル技術とアドレス変換技術の両者を用いる技術の３つがある。

【０００６】なお、ＩＰトンネル技術の一つであるＩＰｓｅｃのトンネルモードは、閉域網内からのＩＰパケットに広域ネットワーク内での転送に使用するＩＰヘッダを付与してカプセル化し、かつ暗号化処理を施すことにより、閉域網間をセキュアに接続する仮想トンネルを作成する技術である。Ｌ２ＴＰでは、端末から公衆電話網を経由して、インターネットプロバイダなどに設置されたアクセスサーバに接続し、さらにこのサーバから閉域網内に用意されたサーバと仮想的なトンネルを確立することにより、端末と閉域網内との間でＰＰＰ（Ｐｏｉｎｔ－ｔｏ－Ｐｏｉｎｔ Ｐｒｏｔｏｃｏｌ）による接続を確立したようなみせるものである。また、ＮＡＴは、ＬＡＮをインターネットに接続する際に、ＬＡＮ側で使用されているプライベートＩＰアドレスをインターネット側で割り当てられているグローバルＩＰアドレスに変換する方法を規定したものである。

【０００７】今、ここにユーザ側閉域網Ａ、Ｂがインターネットを介してサーバ側閉域網ＳにＩＰトンネルを用いて互いの網間アクセスサーバにより接続されているものとする。ユーザ側閉域網Ａ、Ｂに属する各ホストとＳに属するサーバは、それぞれアドレス空間Ａ，Ｂ，Ｓが割り当てられている。この構成により、各ホストは同じ閉域網に属するサーバと接続しているように見せることができる。これにより、各閉域網に割り当てられているローカルアドレスをそのまま使用することが可能になる。しかし、閉域網では、ホストにローカルアドレスを自由に割り当てるので、ユーザ側閉域網間やユーザ側閉域網とサーバ側閉域網間でアドレス空間が重複する場合がある。ユーザ側閉域網間でアドレス空間が重複する場合、サーバから見ると同一のアドレスを持つホストが複数存在していることになり、サーバはどのホストと通信しているのかを正しく認識することができない、という問題が生じる。

【０００８】また、ユーザ側閉域網に属し、ローカルアドレスを割り当てられたホストがインターネット上のグローバルアドレスを割り当てられたサーバと通信を行うためには、そのホストもグローバルアドレスを持つ必要がある。この時、閉域網とインターネットとの境界に設けたＮＡＴ装置にグローバルアドレスを静的に割り当てて、このグローバルアドレスとホストに割り当てられたローカルアドレスとを対応付けることにより、ホストとサーバ間の接続を可能にする。

【０００９】しかし、ＮＡＴ技術は、ローカルアドレスを割り当てられたホストからの接続要求によってそのローカルアドレスとグローバルアドレスとを動的に対応付けて接続の識別を行うために、ホストからの接続要求によって確立されるホストとサーバ間の接続が一旦切断されると、その接続に用いたローカルアドレスとグローバルアドレスとの対応は効力を失ってしまうので、グローバルアドレスを割り当てられたサーバからローカルアドレスを静的に割り当てられたホストへの情報発信などプッシュ型サービスは不可能となる。さらに、サーバは閉域網の識別を行うことができないため、各閉域網に属するホストに対して閉域網に固有のサービスや情報を提供することが困難になる、という問題が生じる。

【００１０】そこで、複数のユーザ側閉域網とサーバ側閉域網とをそれぞれのＩＰトンネルを用いて接続し、ＩＰトンネルを終端するサーバ側閉域網のアクセスサーバにおいて、ユーザ側閉域網のホストとＩＰトンネルのペアに対して固有となるＩＰアドレスを割り当て、これを記憶する。このＩＰアドレスとホストに割り当てられたローカルアドレスとを対応付けることにより、ホストとサーバ間の接続を可能にする。このように、閉域網を特定するアドレス空間の中からホストごとに異なるＩＰアドレスを用いてアドレスの変換を行うため、接続してくるユーザ側閉域網間でのローカルアドレス空間の衝突回避やサーバから特定ホストへの接続を可能にしている。

【００１１】しかし、それぞれのユーザ側閉域網では、サーバが自分らの網内に属しているかのように自由なロ

ーカルアドレスを用いてサーバにアドレスを割り当てることは許されない。他のユーザ閉域網に使用されているローカルアドレス空間や他のユーザ閉域網がサーバへの割り当てを希望しているローカルアドレス空間を考慮した上で、各ユーザ閉域網に固有のサーバアドレスを決定しなくてはならないという問題が生じる。その結果として、物理的に１台のサーバを用いて各ユーザ閉域網にそれぞれ専用サーバがあるかのように動作させるという環境が満たされていない。

【００１２】さらに、ある１つのサーバアプリケーションを各ユーザ閉域網に提供する際に、サーバは共通のサーバプロセスを用いて全てのユーザ閉域網に提供を行っていることが多く、サーバ内部におけるユーザ閉域網の分離はサーバに接続してくるアドレスの違いによってのみ行われるため、サーバを介して他のユーザ閉域網をまたぐ等の不正アクセスの防止ができなくなるとともに、サーバおよびサーバ上で実行されるサーバアプリケーションが常にアドレスの違いを意識したカスタマイズを強要されるので、設定する箇所が非常に多くなり、その結果、閉域網の追加や網構成の変更が困難になる、という問題が生じる。

【００１３】

【発明が解決しようとする課題】従来、インターネット通信においては、ＴＣＰ／ＩＰプロトコル群がホストやルータなどの機器の間での通信に使用されている。そのＴＣＰ／ＩＰプロトコル群はインターネットプロトコルスタックと呼ばれる。このプロトコルスタックの役割として、サーバ装置の物理ネットワークインタフェースまたは複数の仮想的な論理デバイスインタフェースに割り当てられるＩＰアドレス（サーバアドレス）の保持、パケット配送のための経路（ルーティング）情報の保持、各プロトコルパケットの処理などインターネット環境でのネットワーク通信機能を担う。

【００１４】図２は、従来のインターネットプロトコルスタックを示す図である。物理層およびデータリンク層をさらにリンク層６３は、ハードウェアインタフェース（ドライバを含む）６３２，ＡＲＰ（Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）６３３，およびＲＡＲＰ（Ｒｅｖｅｒｓｅ Ａｄｄｒｅｓｓ Ｒｅｓｏｌｕｔｉｏｎ Ｐｒｏｔｏｃｏｌ）６３１によって構成される。ＡＲＰ６３３は、ＩＰアドレスからそのＩＰアドレスに対応するノードのハードウェアアドレス（ＭＡＣアドレス等）を要求するためのプロトコルであり、ＲＡＲＰ６３１は、これとは逆に、自ノードのＭＡＣアドレスを元に、自ノードのＩＰアドレスを要求するためのプロトコルである。

【００１５】ネットワーク層６２は、ＩＰ処理部６２２，ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ Ｃｏｎｔｒｏｌ Ｍｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）６２３，およびＩＧＭＰ（Ｉｎｔｅｒｎｅｔ Ｇｒｏｕｐ Ｍａｎａｇｅｍｅｎｔ Ｐｒｏｔｏｃｏｌ）６２１によって構成される。ＩＣＭＰ６２３は、ＩＰプロトコルの状態に関する情報を管理するために使用されるプロトコルであり、ＩＧＭＰ６２１はＩＰマルチキャストを実現するためのプロトコルである。

【００１６】トランスポート層６１は、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ）６１２とＵＤＰ（Ｕｓｅｒ Ｄａｔａｇｒａｍ Ｐｒｏｔｏｃｏｌ）６１１によって構成される。ＴＣＰ６１２は、ＩＰの上位プロトコルで、コネクション型で信頼性の高い通信を提供し、ＵＤＰ６１１はコネクションレス型のプロトコルで、信頼性確保のための処理を実施しないため、ＴＣＰに比べ高速に処理できる。アプリケーション層６０は、ユーザプロセス６０１によって、エンドユーザでユーザが直接利用する通信サービスを提供する。

【００１７】従来のサーバ装置には、プロトコルスタックが１つのみ用意されており、このサーバ装置と通信を行うホストやルータは、このプロトコルスタックによって提供されるインターネット通信機能とこのプロトコルスタックを通して提供されるサーバプロセスとを共有して利用している。　従って、複数のユーザ側ネットワークに対してサーバサービスを展開するサーバ装置の場合、その多くがユーザ側ネットワークごとに区別してサービスを行わなければならないために、サーバ装置において、ユーザ側ネットワークの特定と分離が必要である。

【００１８】従来のサーバ技術では、サーバに向けて送信されるパケットの送信元アドレスや送信先アドレスの違いを利用してユーザ側ネットワークの特定と分離を行うが、ユーザ側ネットワークがローカルアドレス空間を自由に割り当てることができる閉域網により構築されている場合には、閉域網間におけるローカルアドレス空間の衝突を回避するために、アドレスの制限や変換など強制的なアドレス管理を行い、閉域網間の特定と分離を行い易くしている。しかし、サーバ装置のネットワーク通信機能とサーバプロセスとをユーザ側ネットワークの各々に共有して提供することは、アドレス管理等により、閉域網の特徴である閉域性、サーバからの自発的な情報配信であるプッシュ型サービス、閉域網の追加や網構成変更の容易性などのネットワークサービスの実現を難しくしている。

【００１９】そこで、本発明の目的は、これら従来の課題を解決し、複数のユーザ側閉域網がサーバ側閉域網とＩＰトンネルを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ側閉域網に装置する物理的に１台のサーバ装置により提供されるインターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立した提供を可能にし、そのサーバ装置が各々のユーザ側閉域

網に属している専用サーバであるかのような動作を実現することができる複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法およびサーバ装置を提供することにある。

【００２０】

【課題を解決するための手段】上記目的を達成するため、本発明による複数ユーザ側閉域網とサーバ側閉域網間のネットワーク通信方法では、サーバ装置において、サーバプロセス群からプロトコルスタックまでの上位通信フローと、プロトコルスタックから物理ネットワークインタフェースまたは論理デバイスインタフェースまでの下位通信フローとの組み合わせからなる通信フローを複数装備し、この通信フローをユーザ側閉域網ごとに１つずつ割り当てることにより、各ユーザ側閉域網とサーバ間のサーバ内における個々の通信経路をネットワーク上、論理的に分離し、複数被続しているユーザ側閉域網の特定と分離を実現する。

【００２１】本発明のサーバ装置は、各ユーザ側閉域網に割り当てた固有の通信フローを用いて、プロトコルスタックが担うサーバアドレスの保持、パケット配送経路の制御、各プロトコルパケットの処理などのインターネット通信機能とＷｅｂサーバ、ＦＴＰサーバなどのサーバプロセスとを独立して提供し、ユーザ側閉域網間は他のユーザ側閉域網と通信フローを共有されることなく、ネットワーク上、論理的に隔域性を保持したままサーバ装置との通信を実現する。

【００２２】本発明により、複数のユーザ側閉域網がサーバ側閉域網とＩＰトンネルを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ側閉域網に設置する物理的に１台のサーバ装置によって提供されるインターネット通信機能とサーバプロセスとを各ユーザ側閉域網間で共有することなく、そのサーバ装置が各々のユーザ側閉域網に属している専用サーバであるかのように動作することが可能になる。

【００２３】

【発明の実施の形態】以下、本発明の実施例を、図面により詳細に説明する。図１は、本発明のネットワーク間通信方法を実現するシステム概念図である。

（構成）ここでは、通信フローおよび外部接続が３の場合の構成を示している。複数のユーザ側閉域網（Ａ）３１、（Ｂ）３２、（Ｃ）３３がサーバ側閉域網１０との間で、ＩＰトンネルを用いてアクセスサーバ２６、２８、２９、３０により接続を行っている。各ユーザ側閉域網３１～３３に属するホストａ，ｂ，ｃは、サーバ側閉域網１０に設置する物理的に１台のサーバ装置１１からサーバサービスの提供を受ける。なお、サーバ側閉域網１０のアクセスサーバ装置２６のホスティングサービスについては、特開２００１－０１６２５５号公報に記載の『閉域網間接続システムと閉域網間接続方法およびその処理プログラムを記録した記録媒体ならびにホスティングサービスシステム』を参照されたい。

【００２４】サーバ装置１１は、通信フローを２００程度（図中では３個、１２，１３，１４）備えており、各々のプロトコルスタック１９，２０，２１は図２に示すように、従来のインターネットプロトコルスタックと同じである。すなわち、サーバプロセス群１５，１６，１７とＴＣＰ／ＩＰプロトコル群１９，２０，２１とが上位マッピングモジュール１８を介して接続され、これらＴＣＰ／ＩＰプロトコル群１９，２０，２１と論理デバイスインタフェース２３，２４，２５とが下位マッピングモジュール２２を介して接続されている。サーバ装置１１は、論理デバイスインタフェース２３，２４，２５をこれらのプロトコルスタックと同数だけ備えている。

【００２５】サーバ装置１１は論理デバイスインタフェース２３，２４，２５のそれぞれにリンクするプロトコルスタック１９，２０，２１と各プロトコルスタック１９，２０，２１にリンクするサーバプロセス群１５，１６，１７とを組み合わせてできる通信フロー１２，１３，１４により、ユーザ側閉域網３１，３２，３３間をネットワーク上、論理的に分離し、各々のユーザ側閉域網３１，３２，３３に独立したサーバサービスの提供を行う。以下では、各ユーザ側閉域網３１，３２，３３のホストａ，ｂ，ｃがサーバ側閉域網１０に設置されるサーバ装置１１を利用するための実施例について説明する。

【００２６】図３は、本発明における閉域網の識別にＶＬＡＮタグを用いた場合のネットワーク間通信方法の動作説明図である。

（通信準備）それぞれの閉域網３１，３２，３３では、ローカルアドレスを自由に用いて各ホストａ，ｂ，ｃに割り当てており、他の閉域網の存在を知らないものとする。ホストａは、閉域網３１に属しており、ＩＰアドレスＩａ（192.168.1.10）が割り当てられている。ホストｂは閉域網３２に属しており、ＩＰアドレスＩｂ（192.168.1.10）が割り当てられている。また、ホストｃは閉域網３３に属しており、ＩＰアドレスＩｃ（192.168.1.10）が割り当てられている。閉域網３１，３２，３３間では、ローカルアドレス空間が衝突する可能性があるため、本実施例では故意に衝突させている。

【００２７】サーバ側閉域網１０のアクセスサーバ（Ｓ）２６と各ユーザ側閉域網３１，３２，３３のアクセスサーバ（Ａ）２８、（Ｂ）２９、（Ｃ）３０には、グローバルＩＰアドレスとして、それぞれＧｓ（129.60.1.1）、Ｇａ（129.60.2.1）、Ｇｂ（129.60.3.1）、Ｇｃ（129.60.4.1）が割り当てられている。

【００２８】ユーザ側閉域網３１はサーバ装置１１にローカルアドレスＳａ（192.168.1.1）を、ユーザ側閉域網３２はＳｂ（192.168.1.1）を、ユーザ側閉域網３３はＳｃ（192.168.1.1）を割り当てようとしている。各ユーザ側閉域網３１～３３がサーバアドレスにローカルアドレ

ス空間を自由に割り当てる場合、閉域網間でサーバアドレスが衝突する可能性があるため、本実施例においては故意に衝突をさせている。この要求に従い、サーバ装置１１側では、閉域網３１用として割り当てる通信フロー１２の論理デバイスインタフェース２３（dev0）に対してサーバアドレスＳａ（192.168.1.1）を、閉域網３２用として割り当てる通信フロー１３の論理デバイスインタフェース２４（dev1）に対してサーバアドレスＳｂ（192.168.1.1）を、閉域網３３用として割り当てる通信フロー１４の論理デバイスインタフェース２５（dev2）に対してサーバアドレスＳｃ（192.168.1.1）を、それぞれ割り当てる。

【００２９】このとき、図３に示す下位マッピングモジュール２２では、論理デバイスインタフェース２３，２４，２５とプロトコルスタック１９，２０，２１との間の下位通信フローを管理し、プロトコルスタック１９，２０，２１を該当する論理デバイスインタフェース２３，２４，２５にリンクさせると同時に、それぞれ下位通信フローを構成するプロトコルスタック１９，２０，２１と論理デバイスインタフェース２３，２４，２５とのペア、およびこの下位通信フローを利用する閉域網の代わりとなるＶＬＡＮ（Ｖｉｒｔｕａｌ　ＬＡＮ）タグ３４，３５，３６をセット｛（ｉｎｅｔ0，ｄｅｖ0）⇔ｖｌａｎ600｝，｛（ｉｎｅｔ1，ｄｅｖ1）⇔ｖｌａｎ601｝，｛（ｉｎｅｔ2，ｄｅｖ2）⇔ｖｌａｎ602｝にして、テーブルに記憶する。つまり、ＶＬＡＮタグ３４，３５，３６の値が閉域網を識別する。従来のサーバ装置では、インターネットプロトコルスタックを１つしか持たないため、複数の論理デバイスインタフェースに対して同じサーバアドレスを割り当てることはできなかったが、本発明においては、プロトコルスタックを複数装備することにより、これを可能にしている。

【００３０】次に、各ユーザ側閉域網３１，３２，３３がサーバ装置１１をＷｅｂサーバとして利用することを考える。サーバ装置１１は、サーバプロセス１５，１６，１７がどの閉域網によって利用されるかをプロセスのグループＩＤにより認識する。ユーザ側閉域網３１にはグループＩＤ｛ｇｉｄ1000｝、ユーザ側閉域網３２にはグループＩＤ｛ｇｉｄ1001｝、ユーザ側閉域網３３にはグループＩＤ｛ｇｉｄ1002｝を割り当て、各閉域網３１，３２，３３が利用するＷｅｂサーバのサーバプロセスはそれぞれに割り当てられるグループＩＤを以って実行される。このとき、図３に示す上位マッピングモジュール１８では、サーバプロセス群１５，１６，１７とプロトコルスタック１９，２０，２１との間の上位通信フローを管理し、サーバプロセス１５，１６，１７を該当するプロトコルスタック１９，２０，２１にリンクさせると同時に、それぞれの上位通信フローのプロトコルスタックとグループＩＤとのペア｛ｉｎｅｔ0⇔ｇｉｄ1000｝、｛ｉｎｅｔ1⇔ｇｉｄ1001｝、｛ｉｎｅｔ2⇔ｇｉｄ1002｝をテーブルに記憶する。

【００３１】以上で、上位通信フローと下位通信フローとの組み合わせによってできる通信フロー１２，１３，１４の準備が各ユーザ側閉域網３１，３２，３３に対して完了する。以下では、各ユーザ側閉域網３１，３２，３３のホストａ，ｂ，ｃがサーバ側閉域網１０に設置されるサーバ装置１１と通信を行う方法について説明する。

【００３２】（通信動作）

（ユーザ側閉域網のホストからサーバ装置へ）ユーザ側閉域網３１，３２，３３に属する各ホストａ，ｂ，ｃがＷｅｂサーバとしてのサーバ装置１１と通信することを考える。まず、ホストａは、閉域網３１内に構築したローカルなＤＮＳ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｙｓｔｅｍ）によりサーバ側閉域網１０に属するサーバ装置１１のローカルアドレスＳａを取得する。そして、アクセスサーバ（Ａ）２８に向けてパケットを送信する。他のホストｂ，ｃも、同様にそれぞれアクセスサーバ（Ｂ）２９，（Ｃ）３０に向けてパケットを送信する。

【００３３】ホストａからパケットを受け取ったアクセスサーバ（Ａ）２８は、ＩＰトンネリング処理を行う。すなわち、ホストａのＩＰアドレスＬａとサーバアドレスＳａとを含むＩＰパケットヘッダをアクセスサーバ（Ａ）２８、（Ｓ）２６のグローバルアドレスでカプセル化し、インターネットを経由してアクセスサーバ（Ｓ）２６にパケットを送信する。他のアクセスサーバ（Ｂ）２９、（Ｃ）３０においても、同様の処理が行われ、それぞれがアクセスサーバ（Ｓ）２６にトンネリングされたパケットを送信する。

【００３４】アクセスサーバ（Ａ）２８からパケットを受け取ったアクセスサーバ（Ｓ）２６は、カプセルを解くと、ここから先の通信においてパケットの送信元である閉域網３１を特定可能にするため、ＩＰトンネルとＶＬＡＮタグのペア｛（Ｇａ，Ｇｓ）⇔ｖｌａｎ600｝をテーブルに記憶しており、該当するタグ（ｖｌａｎ600）をパケットに付与する。そして、脱カプセル後のＩＰヘッダに従い、サーバ装置１１に向けてパケットを送信する。このとき、閉域網３２に属するホストｂ、閉域網３３に属するホストｃからの通信も全く同様である。それぞれのＩＰトンネルとＶＬＡＮタグのペア｛（Ｇｂ，Ｇｓ）⇔ｖｌａｎ601｝，｛（Ｇｃ，Ｇｓ）⇔ｖｌａｎ602｝を記憶したテーブルに従って、それぞれＶＬＡＮタグ（ｖｌａｎ601）と（ｖｌａｎ602）がパケットに付与される。

【００３５】アクセスサーバ（Ｓ）２６からタグ付きパケットを受け取ったサーバ装置１１では、そのＶＬＡＮタグ（ｖｌａｎ600）にマッチするプロトコルスタック１９と論理デバイスインタフェース２３のペア｛ｉｎｅｔ0，ｄｅｖ0｝を下位マッピングモジュール２２のテーブルより選択し、該当する通信フロー１２へパケットを転送する。その通信フロー１２の中で、パケットは論理デバイスインタフェース（ｄｅｖ0）２３からプロトコルスタック（ｉｎ

11

et0）１９までの下位通信フローを経由し、同プロトコルスタック１９にリンクされているＷｅｂサーバのサーバプロセス（gid1000）１５へ上位通信フローを使って届けられる。このとき、ホストｂ、ホストｃからの通信も、全く同様のプロセスにより処理される。

【００３６】以上、サーバ装置１１にとって、Ｌａ、Ｌｂ、Ｌｃのように送信元のＩＰアドレスが衝突しても、また各々のユーザ側閉域網３１，３２，３３が割り当てたサーバアドレスがＳａ，Ｓｂ，Ｓｃのように衝突しても、サーバ装置１１内部において通信フロー１２，１３，１４をネットワーク上、論理的に分離しており、サーバサービスを各閉域網３１，３２，３３と全く独立して提供することができる。

【００３７】（通信動作）

（サーバ装置からユーザ側閉域網のホストへ）次に、Ｗｅｂサーバがホストａに返答パケットを送信することを考える。Ｗｅｂサーバのサーバプロセス（gid1000）１５は、自らがリンクしているプロトコルスタック（inet0）１９に対して上位通信フローを使ってパケットを返す。同プロトコルスタック１９の各プロトコルにおいてパケット処理が行われた後、下位通信フローを管理する下位マッピングモジュール２２のテーブル｛（inet0，dev0）⇔vlan600｝に従って、パケットにはＶＬＡＮタグ（vlan600）がタグ付けされ、下位通信フローの論理デバイスインタフェース（dev0）２３からアクセスサーバ（Ｓ）２６に向けてパケットを送信する。このとき、ホストｂ、ｃに対する返答パケットも、全く同様のプロセスにより処理される。

【００３８】サーバ装置１１からタグ付きパケットを受け取ったアクセスサーバ（Ｓ）２６は、ＩＰトンネルとＶＬＡＮタグのペア｛（Ga,6s）⇔vlan600｝を記憶したテーブルに従って、ＩＰトンネリング処理を行う。すなわち、サーバアドレスＳａとホストａのＩＰアドレスＬａとを含むＩＰパケットヘッダをアクセスサーバ（Ｓ）２６、（Ａ）２８のグローバルアドレスでカプセル化し、インターネットを経由してアクセスサーバ（Ａ）２８にパケットを返信する。このとき、ホストｂ，ｃに対する返答パケットも全く同様であり、ＩＰトンネルとＶＬＡＮタグのペア｛（Gb,6s）⇔vlan601｝、｛（Gc,Gs）⇔vlan602｝に従って、アクセスサーバ（Ｂ）２９、（Ｃ）３０にそれぞれパケットを送信する。

【００３９】アクセスサーバ（Ｓ）２６からパケットを受け取ったアクセスサーバ（Ａ）２８は、カプセルを解くと、脱カプセル後のＩＰヘッダに従い、ホストａに向けてパケットを送信する。最終的にホストａがパケットを受け取る。同様に、ホストｂはアクセスサーバ（Ｂ）２９から、ホストｃはアクセスサーバ（Ｃ）３０からパケットを受け取る。

【００４０】（新たなユーザ側閉域網に対するサービス展開）既に登録されているユーザ側閉域網（Ａ）３１，（Ｂ）３２，（Ｃ）３３に対して、新たにユーザ側閉域網（Ｄ）が追加登録された場合、サーバ側閉域網１０では下記のように対処する。未使用の通信フローの中から１つを選び、

（１）プロトコルスタック：（inet3）

（２）グループＩＤ：{gid1003}

（３）上位マッピングモジュール：｛inet3⇔gid1003｝

（４）下位マッピングモジュール：｛(inet3,dev3)⇔vlan603｝

（５）アクセスサーバ（Ｓ）：｛Gd,6s）⇔vlan603｝

を施すことにより、他の閉域網の環境を変更することなく、容易に新たなユーザ側閉域網（Ｄ）に対して仮想サーバサービスを展開することができる。

【００４１】（サーバ装置）図４は、本発明の一実施例を示すサーバ装置の構成図である。図４に示すように、本発明のサーバ装置１１は、複数のプロセスを処理するサーバプロセス４１と、サーバプロセス群からプロトコルスタック多重構成部４６までの上位通信フローを管理する上位マッピングモジュール４２と、プロトコルスタック多重構成部４６から物理ネットワークデバイス多重構成部５１までの下位通信フローを管理する下位マッピングモジュール４７とから構成される。上位マッピングモジュール４２と下位マッピングモジュール４７は、いずれも組み合わせ記憶部４４，４９と、これに結合されたリンク制御部４３，４５および４８，５０から成る。

【００４２】サーバ装置１１は、サーバプロセス４１からプロトコルスタック４６までの上位通信フローと、プロトコルスタック４６から物理ネットワークインタフェースまたは論理デバイスインタフェース５１までの下位通信フローとの組み合わせからなる通信フローを複数装備する。これらの通信フローをユーザ側閉域網ごとに１つずつ割り当てることにより、各ユーザ側閉域網とサーバ装置間のサーバ内における個々の通信経路をネットワーク上で論理的に分離し、複数接続しているユーザ側閉域網の特定と分離を実現している。

【００４３】サーバ装置１１は、各ユーザ側閉域網に割り当てた固有の通信フローを用いて、プロトコルスタック多重構成部４６が担うサーバアドレスの保持、パケット配送経路の制御、各プロトコルパケットの処理などのインターネット通信機能と、Ｗｅｂサーバ、ＦＴＰ（File Transfer Protocol）サーバなどのサーバプロセスとを独立して提供し、ユーザ側閉域網間は他のユーザ側閉域網と通信フローを共有されることなく、ネットワーク上、論理的に閉塞性を保持したまま、サーバ装置１１との通信を行うことが可能である。

【００４４】このように、物理的には１台のサーバ装置１１であるが、サーバプロセス４１がリンク制御部４５により制御されることにより、複数のサーバプロセス群となり、さらにリンク制御部４３の制御により、プロト

コルスタック多重構成部４６が複数のプロトコルスタックを構成する。上位マッピングモジュール４２は、サーバプロセス番とプロトコルスタックとの組み合わせを記憶するとともに、サーバプロセスを該当するプロトコルスタックにリンク制御することにより、上位通信フローを管理する。また、下位マッピングモジュール４７は、物理ネットワークインタフェースまたは論理デバイスインタフェースの多重構成部５１とプロトコルスタック４６との組み合わせを記憶するとともに、プロトコルスタックを該当する物理ネットワークインタフェースまたは論理デバイスインタフェースにリンク制御することにより、下位通信フローを管理する。さらに、上位通信フロー…と下位通信フロー…との組み合わせからなる通信フロー…を複数装備し、これらの通信フロー…をユーザ側閉域網ごとに１つずつ割り当てることにより、各ユーザ側閉域網とサーバ装置間の個々の通信経路をネットワーク上、論理的に分離する。

【００４５】〈サーバ装置用プログラム〉図４および段落番号〔００４１〕～〔００４４〕で説明したサーバ装置の動作をプログラムに変換し、変換したプログラムをＣＤ…ＲＯＭなどの記録媒体に記録しておけば、サーバ側閉域網の任意のサーバ装置のコンピュータにこの記録媒体を装着し、プログラムをインストールして実行させることにより、本発明を容易に実現することができる。

【００４６】

【発明の効果】以上説明したように、本発明によれば、複数のユーザ側閉域網がサーバ側閉域網と１Ｐトンネルを用いてアクセスサーバにより接続を行うネットワーク通信において、サーバ装置により提供されるサーバ機能とサーバプロセスと各ユーザ側閉域網間で共有することなく、各々のユーザ側閉域網に独立して提供することができる。その結果、サーバ閉閉域網に設置する物理的に１台のサーバ装置が各々のユーザ側閉域網に属している専用サーバであるかのように動作させることが可能になる。その結果、今後増加すると予想される複数企業間でのデータ交換を必要とするプロジェクトの実施時や調達業務の実施時に必要となる複数閉域網向けの共用サーバの構築、運用などを提供するハウジングサービスへの展開が可能となる。

【００４７】また、このサービスは、自社の閉域網に手を加えることなく、複数の他企業と情報の連携が可能になるため、ＩＳＰなどが行っているＶＰＮサービスの新しい付加サービスとしての展開が見込める。さらに、企業のみならず、個人向けのポータルサイトサービスへの展開も可能になる。また、本発明では、１つのサーバ装置に対して、各ユーザ閉域網の管理者は、自由にアドレスを付与することができ、プッシュプル型サービスを受けることができる。このように、本発明は、閉域網向けの新しい情報流通プラットフォームを構築する手段としての利用を見込める、という顕著な効果を奏する。

【図面の簡単な説明】

【図１】本発明のネットワーク閉通信方法を適用するネットワーク構成図である。

【図２】従来のインターネットプロトコルスタックを示す図である。

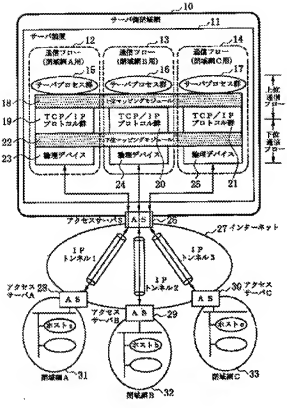
【図３】本発明の一実施例を示すネットワーク閉通信方法の動作説明図である。

【図４】本発明の一実施例を示すサーバ装置の構成図である。

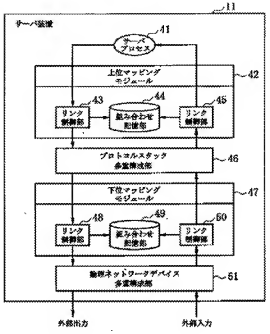
【符号の説明】

１０…サーバ側閉域網、１１…サーバ装置、１２…通信フロー（閉域網Ａ用）、１３…通信フロー（閉域網Ｂ用）、１４…通信フロー（閉域網Ｃ用）、１５，１６，１７…サーバプロセス群、１８…上位マッピングモジュール、１９，２０，２１…ＴＣＰ／ＩＰプロトコル群、２２…下位マッピングモジュール、２３，２４，２５…論理デバイスインタフェース、２６…アクセスサーバ（Ｓ）、２７…インターネット、２８，２９，３０…アクセスサーバ(Ａ),(Ｂ),(Ｃ)、ａ，ｂ，ｃ…ホスト、３１，３２，３３…閉域網（Ａ），（Ｂ），（Ｃ）、３４，３５，３６…ＶＬＡＮタグ、４１…サーバプロセス、４２…上位マッピングモジュール、４３，４５…リンク制御部、４４…組み合わせ記憶部、４６…プロトコルスタック多重構成部、４７…下位マッピングモジュール、４８，５０…リンク制御部、４９…組み合わせ記憶部、５１…論理ネットワークデバイス多重構成部。

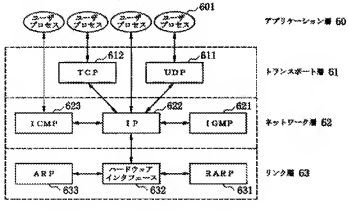
【図１】


10
サーバ仮想領域
11
サーバ装置
12
通信フロー（領域網A用）
13
通信フロー（領域網B用）
14
通信フロー（領域網C用）
15
サーバプロセス群
16
サーバプロセス群
17
サーバプロセス群
18
マッピングモジュール
19
TCP/IP プロトコル群
TCP/IP プロトコル群
TCP/IP プロトコル群
22
プロトコルスタック
23
物理デバイス
物理デバイス
物理デバイス
24
20
25
21
上位通信プロトコル
下位通信プロトコル
アクセスサーバB
AS
26
27 インターネット
IP トンネル1
IP トンネル2
IP トンネル3
アクセスサーバA
28
AS
アクセスサーバC
30
AS
アクセスサーバB
29
AS
ホストA
ホストB
ホストC
領域網A
31
領域網B
32
領域網C
33

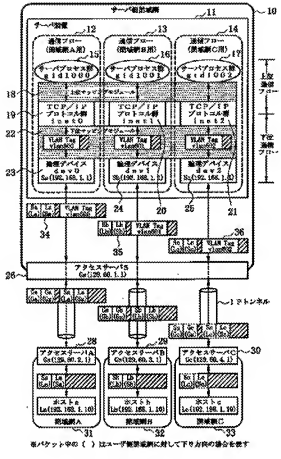
【図４】


11
サーバ装置
41
サーバプロセス
上位マッピングモジュール
42
43
リンク制御部
44
組み合わせ記憶部
45
リンク制御部
プロトコルスタック参照構成部
46
下位マッピングモジュール
47
48
リンク制御部
49
組み合わせ記憶部
50
リンク制御部
物理ネットワークデバイス参照構成部
51
外部出力
外部入力

【図２】


601
ユーザプロセス
ユーザプロセス
ユーザプロセス
ユーザプロセス
アプリケーション層 60
612
TCP
611
UDP
トランスポート層 61
623
ICMP
622
IP
621
IGMP
ネットワーク層 62
ARP
ハードウェアインタフェース
RARP
リンク層 63
633
632
631

【図３】



フロントページの続き

Ｆターム(参考)　5B089 GB01 HB02 HB11 KB06 KF06
KG08
5K033 AA04 CB08 DA05 DB12 DB14